INFORMATION ASSURANCE TECHNOLOGY ANALYSIS CENTER

Information Assurance Tools Report

Winter 97/98

INTRUSION DETECTION

"Building the Knowledge-Base for Emerging Technologies"

8283 Greensboro Drive, Allen 663
McLean, VA 22102-3838

703.902.3177

Fax 703.902.3425

STU-III 703.902.5869

STU-III Fax 703.902.3991

E-mail iatac@dtic.mil

http://www.iatac.dtic.mil

Intelink-S: http://204.36.65.5/index.html

Intelink: http://www.web1.rome

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** Winter 97/98	**3. REPORT TYPE AND DATES COVERED** Winter 97/98

4. TITLE AND SUBTITLE
Information Assurance Technology Analysis Center
Information Assurance Tools Report
Intrusion Detection

5. FUNDING NUMBERS
SPO700-97-R-0603

6. AUTHOR(S)
IATAC

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC/AI
8725 John J. Kingman Road, #0944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
N/A

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This report provides an index of intrusion detection tool descriptions contained in the IATAC Information Assurance Tools Database. This report summarizes pertinent information, so that users can obtain a brief description of available tools and contact information. As a living document, this report will be updated periodically as additional information is entered into the Information Assurance Tools Database

14. SUBJECT TERMS

Intrusion Detection

15. NUMBER OF PAGES
43

16. PRICE CODE None

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** U

TABLE OF CONTENTS

INTRODUCTION

The Information Assurance Technology Analysis Center (IATAC) is a Department of Defense (DoD)-sponsored Information Analysis Center (IAC) that provides a central point of access for Scientific and Technical Information (STINFO) regarding Information Assurance (IA) technologies, system vulnerabilities, research and development, models and analyses. The overarching goal of the IAC is to aid in developing and implementing effective defenses against Information Warfare attacks. IATAC core functions, however, include support for user inquiries, analysis, maintenance, and growth of the IA library; IA database operations; development of technical and state-of-the-art reports; and promotional awareness activities, such as newsletters, conferences, and symposia.

IACs are staffed by scientists, engineers, and information specialists. Each IAC establishes and maintains comprehensive knowledge bases that include historical, technical, scientific, and other data and information collected worldwide. Information collections span a wide range of unclassified, limited distribution, and classified information appropriate to the requirements of sponsoring technical communities. IACs also collect, maintain, and develop analytical tools and techniques including databases, models, and simulations. Their collections and products represent intensive evaluation and screening efforts to create authoritative sources of evaluated data.

The Information Assurance Tools Database is one of the knowledge bases maintained by IATAC. The Information Assurance Tools Database hosts information on intrusion detection, vulnerability analysis, firewalls, and antivirus software applications. Information for this database is obtained via open source methods, including direct interface with various agencies, organizations, and vendors.

PURPOSE

This unclassified report provides an index of intrusion detection tool descriptions contained in the IATAC Information Assurance Tools Database. This report summarizes pertinent information, so that users can obtain a brief description of available tools and contact information. It does not endorse or evaluate the effectiveness of each tool.

As a living document, this report will be updated periodically as additional information is entered into the Information Assurance Tools Database. Technical questions concerning this report may be addressed to James Green at (703) 902-4887 or iatac@dtic.mil.

SCOPE

Intrusion Detection is a broad field of study with elements ranging from motion sensors to real-time electronic intrusion detection systems. The International Computer Security Association (ICSA) defines Intrusion Detection as

"the detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network." [i]

An intrusion attempt is a deliberate, unauthorized attempt to access or manipulate information or render a system unreliable or unusable. The purpose of Intrusion Detection is to decrease the potential magnitude of the compromise or prevent it altogether.

Currently the IATAC database contains descriptions of many tools that detect non-physical intrusions on digital electronic components. The database, which consists of information for 43 tools, includes commercial products, government-owned systems and research products. The database was built by gathering as much open source data as possible, analyzing that data, and summarizing information regarding the basic description and contact information for each intrusion detection tool collected. The existing database does not include pricing and availability information for all of the available tools. Generally, the commercially developed products are available to all domestic interests, while the government and academic tools are reserved for specific projects and organizations. The availability of these research tools is determined by the research group or university on an individual case basis. These tools are included in the database solely to provide information regarding existing approaches for intrusion detection.

DATABASE FORMULATION

This section discusses the approach and methodology used for identifying and collecting the selected tools, the classification of each type, tool sources and the structure of the database.

TOOL COLLECTION

Information for each tool was collected through a variety of means. In one method, the IA community was surveyed via the Internet to identify corporations, government agencies, professional organizations, and universities with involvement in Intrusion Detection. Industry professionals were also consulted for information and suggestions for identifying and collecting available tools. In cases where the accuracy, detail, or date of the information on the collected tools was questionable, the appropriate entities were contacted to validate questionable data.

TOOL CLASSIFICATION

Classification of Intrusion Detection tools in the database required that tools be assigned to one or more classes based on how they operate. The classes are not necessarily discrete; the classes may overlap in various contexts. Therefore, some of the individual classes may appear to be similar, but a distinction was made to more clearly identify the types of tools.

All of the tools share the following twofold problem:

False Positive They must attempt to detect all intrusions while avoiding detecting nonintrusions as intrusions.

False Negative They sometimes do not detect intrusions that, in fact, are intrusions.

The manner in which the various tools attempt to solve these two problems needs to be considered when Intrusion Detection tools are being evaluated. The Intrusion Detection tool descriptions contained in the IATAC Information Assurance Tools Database fall within one or more of the following five classes:

Anomaly Detection Anomaly detection techniques assume that all intrusive activities are a deviation from the norm. These tools typically establish a normal activity profile and then maintain a current activity profile for a system. When the two profiles vary by statistically significant amounts, an intrusion attempt is assumed.

Attack Detection Attack detection systems are based on the concept that there are ways to represent attacks as a pattern or a "signature" so that even variations of the same attack can be detected. These systems maintain records or representations of the actions that represent known bad behavior and identify actions on the system(s) that match the known bad behavior.

File Integrity Checking File integrity checking systems use a cryptographic mechanism to create a unique identifier for each file to be monitored. The identifiers are then stored for future use. Either automatically or manually, the file integrity program is subsequently executed, and new unique identifiers are calculated. The new identifiers are compared with the saved version, and when a mismatch occurs, the integrity checker notifies the operator or administrator that the file has been modified, or deleted. The operator or administrator may then determine if the differences indicate intrusive activity.

Misuse Detection Misuse detection systems attempt to identify authorized users' misuse of computing resources. Such activity may include visiting unauthorized Internet sites, navigating around a system to areas that have been explicitly identified as "off-limits," or using an application for non-work-related activity. Misuse detection systems typically rely on an administrator defining activity that is considered misuse through the use of configuration files. The information in the configuration files can then be compared with activity that occurs on the system; misuse is assumed when there is a match between the two. Misuse detection differs from attack detection in that the later focuses on identifying active attacks against a system whereas the former attempts to identify benign or intentional unauthorized system use.

System Monitoring Detection System monitoring detection either uses available system statistics or generates its own statistical information. These statistics may be derived from various sources, such as central processing unit (CPU) usage, disk input/output (I/O), memory usage, user activity, and number of logins attempted. The statistics are sampled to determine a normal system usage profile and are continually updated to reflect the current system state. The current state is compared with the normal usage state and the Intrusion Detection System determines whether the actions that have changed the profiles/states constitute a potential intrusion.

The foregoing classifications highlight the differences among the tools. However, the methods used by the different tools are also similar in many respects. Those methods listed below describe the data sources and activities that the tools use to detect intrusions. Methods that could be used by one or more of the tools include the following:

Audit-Based Detection An audit-based detection system has two major components. One is a catalog of audited events that are considered "bad" behavior. This data could include attack profiles, suspicious activity profiles, and defined unacceptable activities. The second component is an audit trail analysis module. Audit trails from a chronological record of activities on a system. The analysis module examines the monitored system's audit trail for activity that matches activity in the catalog; when a match occurs, intrusive activity is assumed. Audit-based systems may also provide the ability to identify and track additional activity that has been performed by an individual suspected of intrusive activity.

Expert Systems Detection Expert systems are designed to act when a given situation occurs. The system often chains such activities so that when one situation occurs, it causes an action that may result in another situation that may cause another action. This pattern could occur many times before the sequence is complete. The difference between the expert system method and the methods that use catalogs of information and match activity to entries is that the nonexpert systems compare only discrete activity to discrete information and then perform an action. Expert systems can group activities and events together to make comparisons.

Keystroke Monitoring Detection Like, audit-based detection, keystroke monitoring technique consists of two components. Like the audit-based technique, a catalog of "bad" behavior is maintained. In this case, however, the catalog is of specific keystrokes that indicate attacks. The second component is a module that captures keystrokes as they are entered by the user and then compares them with the catalog. When entered keystrokes match a catalog entry, an intrusion is assumed.

State Transition Analysis The State Transition Analysis technique represents the monitored system as a state transition diagram. As incoming data is analyzed, the system transitions from one state to another. A transition depends on a particular Boolean condition becoming true (for example, the user's opening a file). Intrusions are assumed when the system transitions from a safe to an unsafe state, based on known attack patterns contained in the intrusion detection tool.

TOOL SOURCE

Tools were identified from a number of sources. A representative sampling of these sources includes the following:

COMMERCIAL PRODUCT OFFERINGS

Axent Technologies

Cisco Systems

Digital Equipment Corporation

En Garde Systems

Fischer International Systems Corporation

Harris Corporation

Haystack Laboratories

Internet Security Systems

Intrusion Detection Incorporated

Los Altos Technologies

MimeStar

Network General Corporation

Science Applications International Corporation

SRI International

SUPELEC

Touch Technologies

Trident Data Systems

WheelGroup Corporation

ACADEMIA RESOURCE CENTERS

Brandenburg University of Technology at Cottbus University

Carnegie Mellon University, Software Engineering Institute

Columbia University, Department of Computer Science

Curtin University of Technology

Marquette University

Massachusetts Institute of Technology

Microelectronics Center of North Carolina (MCNC)

Purdue University, Autonomous Agents

Stanford University

Texas A&M University

TU Braunschweig

University College Dublin, Security Research Group

University of California at Davis

University of California at Santa Barbara

University of Hamburg

University of Illinois

University of Namur

University of New Mexico

GOVERNMENT AND PROFESSIONAL AGENCIES AND RESEARCH CENTERS

Air Force Information Warfare Center

Defense Information Systems Agency (DISA)

Department of Energy, Computer Incident Advisory Capability (CIAC)

International Computer Security Association (ICSA)

Lawrence Berkeley National Laboratory

Lawrence Livermore National Laboratory

Los Alamos National Laboratory

National Institute of Standards and Technology (NIST)

U.S. Army Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4)

U.S. Navy Space and Naval Warfare Systems Command (SPAWAR)

DATABASE STRUCTURE

The fields of the database include the following:

Title Name and abbreviation associated with the tool

Author Developer of the tool, listed by organization (company, agency, university, etc.) and/or individual(s) associated with the development

Source Uniform resource locator (URL) of the primary source for the abstract information

Keywords Terms used to reference the tools using the database search engine

Contact Information Name, organization, telephone, facsimile, email, and URL information for further tool information

Abstract Brief description of the primary features of the tool

Bibliography Reference sources for comments and information

TOOL SELECTION CRITERIA

The selected tools satisfy the following three criteria:

Definition These tools satisfy the objective, approach and methodology of an Intrusion Detection Tool based upon the ICSA definition of Intrusion Detection, as described in Section 3 of this report.

Specificity to Intrusion Detection The primary function of these tools is Intrusion Detection, not penetration testing or vulnerability analysis. Intrusion detection differs from penetration tests in that detection aims to identify attacks while penetration tests concentrate on the security architecture and policies of a system. Penetration tests exploit system and user vulnerabilities. Vulnerability analysis differs from intrusion detection and penetration tests in that vulnerability tools focus on exposing common or "known" weaknesses.

Current Availability These tools are currently available; some on a limited basis, and for some cost, from the government, academia, or commercial arenas.

RESULTS

The research for this report identified 43 Intrusion Detection tools currently being used and available. Appendix A includes complete database output for each tool. The content of Appendix A mirrors the database structure as defined is Section 4.4 of this report. The following summary chart provides the name, keywords, and a description of each tool.

[i] *International Computer Security Association. Glossary of Firewall Related Terms. http://www.ncsa. com/ fwpg_p8.html, November 21, 1997.*

SUMMARY OF INTRUSION DETECTION TOOLS

Title	Source Type	Attributes	Contact Organization	E-mail	URL
ADS	Academia	attack detection	University College, Dublin	ciaranc@net-cs.ucd.ie	www.ucd.ie
AID	Academia	audit-based, misuse detection	Brandenburg University	sobirey@informatik.tu-cottbus.de	www-rnks.informatik. tu-cottbus.de/~sobirey
ALVA	Individual	anomaly detection, audit-based	Abha Moitra	moitraa@crd.ge.com	www.crd.ge.com/rd18.html
Argus	Academia	audit-based, system monitoring	Carnegie Mellon University	argus@sei.cmu.edu	ftp.sei.cmu.edu/pub
ARPMon	Academia	system monitoring	University of Illinois	gressley@uiuc.edu	flowbee.beckman.uiuc.edu/~gressley
ARPWATCH	Government / Research	system monitoring, spoofing	Lawrence Berkeley National Laboratory	van@ee.lbl.gov	www-nrg.ee.lbl.gov
ASAX	Academia	audit-based, misuse detection	University of Namur	amo@info.fundp.ac.be	www.info.fundp.ac.be/~amo
ASIM	Military	anomaly detection	CAEWIS	mccroan@wg53.eglin.af.mil	www.wg53.eglin.af.mil/53spts/sc/scc/caewis.htm
CMDS	Commercial	anomaly detection, audit-based, expert system, misuse detection	SAIC	cmds@cpqm.saic.com	www.saic.com/it/cmds/index.html
Courtney	Government / Research	system monitoring	CIAC	ciac@llnl.gov	ciac.llnl.gov
CyberCop	Commercial	anomaly detection, misuse detection, system monitoring	Network General Corporation	debh@ngc.com	www.ngc.com
EMERALD	Commercial	anomaly detection, system monitoring	SRI	porras@csl.sri.com	www.csl.sri.com/emerald/index.html
Gabriel	Commercial	system monitoring	Los Altos Technologies	Majordomo@lat.com	www.lat.com/gabe.htm
GrIDS	Academia	anomaly detection, sniffers	University of California at Davis	heberlei@cs.ucdavis.edu	seclab.cs.ucdavis.edu/arpa/people/todd.html
IDES/NIDES	Commercial	anomaly detection, expert system, misuse detection, system monitoring	SRI	porras@csl.sri.com	www.csl.sri.com/~porras
IDIOT	Academia	misuse detection	Purdue University	spaf@cs.purdue.edu	www.cs.purdue.edu/faculty/spaf.html
Ifstatus	Individual	anomaly detection	David Curry	davy@vnet.ibm.com	www.ers.ibm.com/~davy
Internet Scanner Toolset	Commercial	anomaly detection, vulnerability analysis	Internet Security Systems	info@iss.net	www.iss.net
ITA	Commercial	anomaly detection, audit-based, misuse detection	AXENT Technologies	info@axent.com	www.axent.com/about/contact/contact.htm
Kane Security Monitor	Commercial	misuse detection, system monitoring	Intrusion Detection Incorporated	info@intrusion.com	www.intrusion.com/contact.htm
md5check	Academia	file integrity	University of California at Davis	heberlei@cs.ucdavis.edu	seclab.cs.ucdavis.edu/arpa/people/todd.html
NADIR	Government/ Research	anomaly detection	Los Alomos National Laboratory	jlt@lanl.gov	www.lanl.gov/cgi-bin/phone/085768
NETMAN	Academia	system monitoring	Curtin University of Technology	customer-service@curtin.edu.au	www.cs.curtin.edu.au/~mike
NetRanger	Commercial	anomaly detection, misuse detection, system monitoring	WheelGroup Corporation	info@wheelgroup.com	www.wheelgroup.com/contact/1contact.html
NID	Government / Research	anomaly detection, misuse detection	CSTC	IPandC@llnl.gov	ciac.llnl.gov/cstc/nid/nid.html
NIDES	Commercial	anomaly detection, expert system, misuse detection, system monitoring	SRI	porras@csl.sri.com	www.csl.sri.com/~porras
NOCOL	Academia	system monitoring	Marquette University	doug@mscs.mu.edu	www.mscs.mu.edu/contact.html
Noshell	Commercial	system monitoring	CiscoSystems	cs@cisco.com	www.cisco.com/warp/public/437/Service.html
NSM	Academia	system monitoring	University of California at Davis	heberlei@cs.ucdavis.edu	seclab.cs.ucdavis.edu/arpa/people/todd.html
POLYCENTER	Commercial	misuse detection, system monitoring	DEC	polycenter@digital.com	www.digital.com/misc/contacts.txt.html#US
RealSecure	Commercial	vulnerabilityanalysis	ISS	info@iss.net	www.iss.net/prod/rs.html
SecureNet Pro	Commercial	keyword-level surveillance, system monitoring	MimeStar	MimeStar@MimeStar.com	www.mimestar.com/secids.htm

Title	Source Type	Attributes	Contact Organization	E-mail	URL
Stake Out	Commercial	anomaly detection, misuse detection, system monitoring	Harris Corporation	stakeout@harris.com	www.stakeout.harris.com
Stalker	Commercial	misuse detection	Haystack Laboratories	sales@haystack.com	www.haystack.com/contfr.htm
Swatch	Academia	misuse detection, system monitoring	Stanford University	security@Stanford.EDU	www-leland.stanford.edu/group/itss-ccs/security
Tripware	Academia	file integrity	Purdue University	walls@cs.purdue.edu	www.cs.purdue.edu/people/walls
T-sight	Commercial	system monitoring	En Garde Systems	spec@engarde.com	www.engarde.com/contact.html
UNICORN	Commercial	audit-based	En Garde Systems	spec@engarde.com	www.engarde.com/contact.html
USTAT	Academia	misuse detection, state transition analysis	University of California Santa Barbara	kemm@cs.ucsb.edu	www.cs.ucsb.edu/~kemm
WatchDog	Commercial	system monitoring	Fischer International Systems Corporation	Ron.Buehrer@fisc.com	www.fisc.com/store/wd.html
WebStalker Pro	Commercial	misuse detection	Haystack Laboratories	sales@haystack.com	www.haystack.com/contfr.htm
X Connection Monitor	Academia	system monitoring	Purdue University	walls@cs.purdue.edu	www.cs.purdue.edu/people/walls

ADS

TITLE

ADS (Attack Detection System)

AUTHOR

Ciaran Clissmann
University College Dublin, Security Research Group

SOURCE

http://www-rnks.informatik.tu-cottbus.de/~sobirey/idsbibl.html#ADS

KEYWORDS

attack detection

CONTACT INFORMATION

Ciaran Clissmann
University College Dublin, Belfield, Dublin 4, Ireland

Phone:	353.1.706.2485
Fax:	353.1.269.7262
Email:	ciaranc@net-cs.ucd.ie
URL:	http://www.ucd.ie

ABSTRACT

ADS is an attack detection system for secure computer systems. The University College Dublin Security Research Group is researching methods for protecting a network from attack by entities with subversive purposes. The specification of security protocols, research into international security standards, and the provision of security to client programs by a security server are some of the current research areas of the group.

BIBLIOGRAPHY

Kantzavelou, I., Katsikas, S. K.: An attack detection system for secure computer systems - Outline of the solution, in Yngström, L.; Carlsen, J. (eds.). Information Security in Research and Business, Proc. of the IFIP TC11 13th International Information Security Conference (SEC'97), Copenhagen, Denmark, May 1997, Chapman & Hall, London, 123 135.

Kantzavelou, I.; Patel, A.: An attack detection system for secure computer systems - Design of ADS, Katsikas, S. K.; Gritzalis, D. (eds.) Information Systems Security, Proc. of the IFIP TC11 12th International Information Security Conference (SEC'96), May 1996, Samos, Greece, Chapman & Hall, London, 1996, 1 16.

TITLE

AID (Adaptive Intrusion Detection System)

AUTHOR

Michael Sobirey and Birk Richter
Brandenburg University of Technology at Cottbus

SOURCE

http://www-rnks.informatik.tu-cottbus.de/~sobirey/aid.e.html

KEYWORDS

audit-based detection, misuse detection

CONTACT INFORMATION

Michael Sobirey
Brandenburgische TU Cottbus,
Institut für Informatik, Postfach 10 13 44, 03013 Cottbus
Phone: 03.55.69.21.01
Fax: 03.55.69.22.36
Email: sobirey@informatik.tu-cottbus.de
URL: http://www-rnks.informatik.tu-cottbus.de/~sobirey/

ABSTRACT

AID is a distributed intrusion detection system that consists of agents on the monitored hosts and a central monitoring station with an expert system. The monitoring agents collect local audit data and convert them into an operating system-independent data format. The audit data are then transferred to the central monitoring station where an expert system analyzes the data to detect known attack scenarios. The security officer can access relevant monitoring capabilities and generate security reports via a graphical user interface. The prototype AID supports Solaris 2.x.

The development of AID is ongoing at the Brandenburg University of Technology at Cottbus. The system is designed for network audit based monitoring of local area networks and used for investigating network and privacy oriented auditing. The research project was funded by the Brandenburg Department of Science, Research and Culture from 1994 to spring 1996.

The system has a client-server architecture consisting of a central monitoring station and several agents (servers) on the monitored hosts. The central station hosts a manager (client) and an expert system. The agents take the audit data that were collected by the local audit functions and convert them into an operating system-independent data format. By these means a monitoring of a heterogeneous UNIX environment is supported. Then the audit data are transferred to the central monitoring station, buffered in a cache, and analyzed by an Rtworks-based real-time expert system. The manager provides functions for the security administration of the monitored hosts. It controls their audit functions, requests new audit data by controlled polling and returns the decisions of the expert system to the agents. Secure RPC is used for the communication between the manager and the agents.

The expert system uses a knowledge base with state oriented attack signatures, which are modeled by deterministic finite state machines and implemented as rule sequences. Relevant monitoring capabilities can be accessed by the security officer via a graphical user interface. In addition, the expert system archives data on finished and canceled attacks and involved users, and creates security reports.

AID has been successfully tested in a local area network environment consisting of Sun SPARCstations running with Solaris 2.x and TCP/IP. Meanwhile, 100 rules are implemented and the knowledge base is capable of detecting 10 attack scenarios. In the described configuration and under the assumption of normal system load on the monitored hosts (maximum two working users, no patching in progress), the expert system analyzes more than 2.5 MB per minute. The tests have shown that the prototype can monitor up to 8 hosts.

Further development includes privacy-oriented pseudonymous auditing, host-oriented network audit, integration of functions for active defense of detected attacks, adaptions/extensions for monitoring of Windows NT environments, and adaptive anomaly detection using Kohonen Feature Maps.

BIBLIOGRAPHY

Sobirey, M.; Richter, B.; König, H.: The Intrusion Detection System AID. Architecture, and experiences in automated audit analysis, in Horster, P. (ed.): Communications and Multimedia Security II, Proc. of the IFIP TC6 / TC11 International Conference on Communications and Multimedia Security, Essen, Germany, Sept. 1996, Chapman & Hall, London, 278 290.

TITLE

ALVA (Audit Log Viewer and Analyzer Tool)

AUTHOR

Abha Moitra

KEYWORDS

anomaly detection, audit-based detection

CONTACT INFORMATION

Abha Moitra
K1-5C33
GE Corporate R&D
Schenectady, NY 12301
Phone: 518.387.6488
Fax: 518.387.5324
Email: moitraa@crd.ge.com
URL: http://www.crd.ge.com/rd18.html

ABSTRACT

ALVA is a real-time tool for detecting potential security violations in UNIX audit logs. The system gains some level of platform independence by analyzing command logs that are precomputed from the system audit logs. A command log, which is a record of the user initiated commands, is reconstructed from the system call events recorded in the audit log. User's command logs would be similar across UNIX platforms, so processing of the logs would be platform independent across UNIX workstations. A simple profile based on command, success/failure, frequency of occurrence, and the domain of the target files is used to define a baseline of normal behavior for each user. A single penalty value is kept for each user, and when the user crosses a predefined threshold, ALVA reacts by contacting the security administrator and increasing the auditing level for the user. ALVA was developed to run on a C2 security level SUN environment.

BIBLIOGRAPHY

Moitra, A.: Real-time Audit Log Viewer and Analyzer, Proc. of the 4th Workshop on Computer Security Incident Handling (Forum of Incident Response and Security Teams FIRST), Denver, CO, Aug. 1992.

TITLE

Argus 1.5

AUTHOR

Carter Bullard and Chas DiFatta
Carnegie Mellon University

SOURCE

ftp://ftp.sei.cmu.edu/pub/argus-1.5/argus-1.5.announce

KEYWORDS

audit-based detection, system monitoring

CONTACT INFORMATION

Carter Bullard
Chas DiFatta
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412.268.5800
Fax: 412.268.5758
Email: C. Bullard, wcb@sei.cmu.edu
C. DiFatta, chas@sei.cmu.edu
argus@sei.cmu.edu
URL: ftp://ftp.sei.cmu.edu/pub/

ABSTRACT

As a UNIX network monitoring tool, Argus is a generic IP network transaction auditing tool that has allowed Carnegie Mellon University's SW Engineering Institute to perform a number of powerful network management tasks that are currently very difficult using commercial network management tools. It requires the libpcap and tcp_wrappers packages.

Argus and its supporting routines have been developed on SPARC architectures under SunOS 4.1.x, and have been successfully ported to Solaris 2.3 and SGI IRIX5.2. No claim is made as to the portability of Argus to other platforms.

Argus is dependent on the public domain packages libpcap and tcp_wrappers. Libpcap provides the packet capture facility for Argus, and tcp_wrappers provides remote access control. At this time, the latest versions are libpcap-0.0.6 and tcp_wrappers-7.2. It is recommended that because these packages be installed at the same directory level as Argus, because the installation configuration scripts look for them.

TITLE

ARPMon

AUTHOR

Computing and Communications Services Office, University of Illinois at Urbana-Champaign

SOURCE

http://tampico.cso.uiuc.edu/docs/jacques/software/arpmon.html

KEYWORDS

system monitoring

CONTACT INFORMATION

Christine R. Gressley
1714 Beckman Institute, MC-251
405 N. Mathews Ave.
University of Illinois at Urbana-Champaign
Urbana, IL 61801

Phone:	217.244.7371
Fax:	217.333.8206
Email:	gressley@uiuc.edu
URL:	http://flowbee.beckman.uiuc.edu/~gressley

ABSTRACT

Address Resolution Protocol (ARP) is a protocol that maps IP addresses to physical network or hardware addresses. The Jacques ARPmon tools use the ARP to monitor the usage of IP addresses on a network. The ARPmon tools track the date and time when a hardware address last used a particular IP address. In addition, the ARPmon tools monitor and report when a hardware address is using an incorrect IP address.

Because IP addresses do not physically identify individual stations on a network, the ARP protocol was developed to find a host's hardware address by the host's IP address. Each host on a network maintains an ARP table, which is just a list of IP addresses and associated hardware addresses. When a host sends data to another station on the network, first the station searches its ARP table to find the physical hardware address of the destination IP address. If the hardware address is not located in the ARP table, the host sends an ARP broadcast request packet. All stations on the network will receive the packet, but only the station with that IP address will reply with an ARP reply packet. The host sending the ARP request will update its own ARP table upon receiving the ARP reply packet.

A router dynamically builds and maintains a table of translations between IP addresses and hardware addresses using ARP. When the router receives an ARP request to translate an IP address for a host, it checks for the hardware address in its ARP table. If the address is found, it returns the Ethernet address to the requesting client. If the address is not found in the table, ARP broadcasts a packet to every host on the Ethernet. The packet contains the IP address for which an Ethernet address is sought. If the receiving host identifies the IP address as its own, it responds by sending its Ethernet address back to the requesting host the response is then cached. An Ethernet address is removed from the ARP cache after a period of time.

The current mappings of hardware address to IP address are checked against the BOOTP configuration file. Discrepancies between the BOOTP configuration file and the current hardware to IP address mappings obtained via ARP are indicative that a user is using the wrong IP address. Notifications of discrepancies are automatically generated.

TITLE

ARPWATCH 1.3

AUTHOR

LBL Network Research Group
Berkeley, CA

SOURCES

http://cs-www.ncsl.nist.gov/tools/ tools.htm#intrusion

KEYWORDS

spoofing, system monitoring

CONTACT INFORMATION

Van Jacobson
Lawrence Berkeley National Laboratory
1 Cyclotron Rd., 50B-2239
Berkeley, CA 94720
Phone: 510.486.6357
Fax: 510.486.6363
Email: van@ee.lbl.gov
URL: http://www-nrg.ee.lbl.gov

ABSTRACT

This product aims to protect against address spoofing. ARPWATCH monitors Ethernet activity and keeps a database of Ethernet/ip address pairings. It also reports certain changes via email. ARPWATCH uses libcap, a system-independent interface for user-level packet capture. Before TCPdump is built, retrieve and build libpcap, also from LBL, in: ftp://ftp.ee.lbl.gov/libpcap-*.tar.Z.

TITLE

ASAX (Advanced Security audit trail Analysis on UNIX)

AUTHOR

Baudouin Le Charlier, Abdelaziz Mounji, and Naji Habra, University of Namur, Belgium and Isabelle Mathieu, Siemens-Nixdorf Software S.A.

SOURCE

http://www.info.fundp.ac.be/~amo/
publications.html
ftp://ftp.info.fundp.ac.be/pub/projects/asax

KEYWORDS

audit-based detection, misuse detection

CONTACT INFORMATION

Abdelaziz Mounji
Institut d'Informatique
University of Namur
Rue Grandgagnage
21 B-5000 Namur, Belgium
Phone: 32.81.72.49.87
FaX: 32.81.72.49.67
Email: amo@info.fundp.ac.be
URL: http://www.info.fundp.ac.be/~amo/

ABSTRACT

ASAX is a distributed audit trail analysis system that also has incorporated configuration analysis. The audit trail analysis system consists of a central master host and one or more monitored machines. The monitored machines analyze their local audit data using a host-based version of an intrusion detection system, and relevant events are selected to be sent to the central host. The selected events are converted before being transmitted to the central host for global analysis. The conversion allows for global analysis of data from heterogeneous environments. Both the local host-based and global analysis engines are rule-based systems that detect known penetration patterns. This hierarchical model lends itself to detecting components of a pattern at a local level and to deriving the aggregate pattern at the global level. In the latest version of ASAX, configuration analysis has been integrated with the intrusion detection system. By continuously monitoring the current configuration of the system, ASAX has the ability to tune the intrusion detection system to the current system state. The integrated system not only reports newly created security holes in real time, but also triggers appropriate detection rules to watch for exploits of the new holes. ASAX supports audit data from Solaris 2.x.

BIBLIOGRAPHY

Mounji, A. Languages and Tools for Rule-Based Distributed Intrusion Detection PhD Thesis. Computer Science Institute, University of Namur, Belgium, Sept. 1997.

Mounji, A., Le Charlier, B. Continuous Assessment of a UNIX Configuration: Integrating Intrusion Detection and Configuration Analysis. In Proceedings of the ISOC' 97 Symposium on Network and Distributed System Security. San Diego, California, 1997.

Mounji, A., Le Charlier, B. Detecting Breaches in Computer Security: A Pragmatic System with a Logic Programming Flavor In Proceedings of the Eight Benelux Workshop on Logic Programming. September, 1996. Louvain-La-Neuve, Belgium.

Habra, N.; Le Charlier, B.; Mounji, A.; Mathieu, I.: ASAX: Software architecture and rule-based language for universal audit trail analysis, Deswarte, Y.; Eizenberg, G. (eds.): Proc. of the 2nd European Symposium on Research in Computer Security (ESORICS '92), Toulouse, France, Nov. 1992, 435 450.

ASIM

TITLE

ASIM (Automated Security Incident Measurement)

AUTHOR

U.S. Air Force

SOURCE

http://www.senate.gov/~gov_affairs/dem/psi/hearings/960522/gaosum.htm

http://www.infowar.com/civil_de/gaosum.html-ssi#CH3

KEYWORDS

anomaly detection

CONTACT INFORMATION

Peggy McCroan
Computer Aided Electronic Warfare Information System (CAEWIS)
Eglin Air Force Base
Eglin, Florida

Phone:	904.882.9907
Fax:	n/a
Email:	mccroan@wg53. eglin.af.mil
URL:	http://www.wg53.eglin.af.mil/53spts/sc/scc/caewis.HTM

ABSTRACT

The Air Force has a project underway called Automated Security Incident Measurement (ASIM) which is designed to measure the level of unauthorized activity against its systems. Under this project, several automated tools are used to examine network activity and detect and identify unusual network events, for example, Internet addresses not normally expected to access defense computers. These tools have been installed at only 36 of the 108 Air Force installations around the world. Selection of these installations was based on the sensitivity of the information, known system vulnerabilities, and past hacker activity. Data from the ASIM are analyzed by personnel responsible for securing the installation's network. Data are also centrally analyzed at the AFIWC in San Antonio, Texas.

Air Force officials at AFIWC and at Rome Laboratory have found ASIM extremely useful in detecting attacks on Air Force systems. As currently configured, however, ASIM information is only accumulated and automatically analyzed nightly. As a result, a delay occurs between the time an incident occurs and the time when ASIM provides information on the incident. They also stated that ASIM is currently configured for selected operating systems and, therefore, cannot detect activity on all Air Force computer systems. Plans are to continue refining the ASIM to broaden its use for other Air Force operating systems and enhance its ability to provide data on unauthorized activity more quickly. AFIWC officials believe that a well-publicized detection and reaction capability can be a successful deterrent to would-be attackers.

TITLE

CMDS (Computer Misuse Detection System)

AUTHOR

Science Applications International Corporation,
San Diego, CA

SOURCE

http://www.saic.com/it/cmds/index.html

KEYWORDS

anomaly detection, audit-based detection, expert system, misuse detection

CONTACT INFORMATION

Matthew W. Tobriner
SAIC Security Products Division
10260 Campus Point Drive, MS/B-1-P
San Diego, CA. 92121-1578
Phone: 619.552.5250
FaX: 619.552.5251
Email: cmds@cpqm.saic.com
URL: http://www.saic.com/it/cmds/index.html

ABSTRACT

The CMDS™ technology performs real-time audit reduction and analysis to detect and deter computer misuse. It protects against access from Internet users and from insider misuse on heterogeneous networks. With one CMDS server, hosted on a UNIX workstation, a security administrator can monitor and control system access at terminals and IP addresses throughout a network. CMDS technology monitors network wide activities through a TCP/IP connection. It uses a flat file database for speed, a forward-chaining expert system for customization, and an intuitive Windows interface for real-time and historical reporting.

CMDS technology detects computer misuse by calculating expected behavior profiles from historical data and comparing those profiles to normal behavior profiles for each user or IP address, performing real-time analysis on the data, graphically displaying it, and storing all profile data for easy retrieval, reducing the data to comprehensible size and automatically generating reports, storing all raw audit records for future reference. Target machines generate audit data that are passed to the CMDS server. The server processes each audit record through statistical and rule-based filters using serial and parallel methods. For serial operation, statistical calculations assert facts into the knowledge base. For parallel operation, raw data can produce an alert from either the statistical calculations or the rule-based detection modules. Profiles, warnings, and alerts are written to the CMDS database. The CMDS server uses the processed data for real-time displays, alerts, and warnings. Reports are generated from the CMDS database.

The CMDS technology includes three misuse detection mechanisms statistical detection, rule-based detection, trending reports. Statistical detection involves monitoring the network for deviations from expected activity. CMDS monitors and records target system activity and creates a statistical profile, or measurable baseline, for each target user. Using this baseline, CMDS analyzes and measures subsequent target activity. This baseline is calculated through a mean and standard deviation statistical model based on different classes of commands. Using these statistics, CMDS calculates a current behavior profile with commands received in real time. If current behavior deviates beyond a set threshold, CMDS generates a real-time warning to the CMDS console, alerting the security administrator to suspicious activity.

CMDS uses an expert system, CLIPS, and a customized rule base to model misuse scenarios. Facts, or target user or IP address activity, are asserted into the expert system fact base. When activity begins to mirror any of the modeled misuse scenarios within the rule set, CMDS generates a real-time alert or warning to the CMDS console, alerting the security administrator of suspicious activity. Trending reports use data from the profiles, warnings, and alerts in the CMDS database to summarize real-time and historical patterns of computer activity. The administrator can decide what statistical categories of computer behavior and what threshold of activity in each category will trigger a security alert. CMDS notifies the security administrator immediately when suspicious activity takes place.

BIBLIOGRAPHY

Proctor, P.: Audit reduction and misuse detection in heterogeneous environments: Framework and application, Proc. of the 10th Annual Computer Security Applications Conference, Orlando, FL, Dec. 1994, 117 125.

TITLE

Courtney

AUTHOR

Computer Incident Advisory Capability (CIAC), Livermore, CA

SOURCE

ftp://ciac.llnl.gov/pub/ciac/sectools/UNIX/courtney/

KEYWORDS

system monitoring

CONTACT INFORMATION

Sandy Spark
Computer Incident Advisory Capability
University of California
Lawrence Livermore National Laboratory
7000 East Ave. (P.O. Box 808)
Livermore, CA 94550
Phone: 510.422.8193
Fax: 510.423.8002
Email: ciac@llnl.gov
URL: http://ciac.llnl.gov

ABSTRACT

Courtney monitors the network and identifies the source machines of SATAN probes/attacks. Courtney receives input from tcpdump counting the number of new services a machine originates within a certain time window. If one machine connects to numerous services within that time window, Courtney identifies that machine as a potential SATAN host.

TITLE

CyberCop

AUTHOR

Network General Corporation
Dunn Loring, VA

SOURCE

http://www.ngc.com/product_info/cybercop/ccdata/ccdata1.html

KEYWORDS

anomaly detection, misuse detection, system monitoring

CONTACT INFORMATION

Deborah Horan
Channel Manager, Eastern Region
Address: Network General Corporation
2222 Gallows Road, Suite 200
Dunn Loring, VA 22027
Phone: 703.641.0074
Fax: 703.204.9428
Email: debh@ngc.com
URL: http://www.ngc.com

ABSTRACT

CyberCop™ is an intrusion detection system that protects networks by providing full-time monitoring and real-time alarms when suspicious activities are detected. CyberCop detects attacks and misuses from outside the network as well as from within.

CyberCop is a real-time security solution that issues alarms when attacks are identified, recognizes networked elements under attack, logs the activity, and captures evidence of the intrusion.

CyberCop has ease-of-use features that make the product usable by system or network managers. This means that CyberCop is easy to deploy and configure as well as easy to manage and operate. CyberCop's designed-in security means that the system is practically impossible to detect or bring down and will be operational during any attack.

As a network-based solution utilizing distributed sensors, it starts to protect the network with minimal configuration and maximum intelligence.

EMERALD

TITLE

EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances)

AUTHOR

SRI International, Menlo Park, CA

SOURCE

http://www.csl.sri.com/emerald/index.html

KEYWORDS

anomaly detection, system monitoring

CONTACT INFORMATION

Phillip A. Porras
Computer Science Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025
Phone: 650.859.5924
Fax: 650.859.2844
Email: porras@csl.sri.com
emerald@csl.sri.com
URL: http://www.csl.sri.com/emerald/index.html

ABSTRACT

The EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment is a distributed scaleable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. It combines models from research in distributed high-volume event-correlation methodologies with over a decade of intrusion detection research and engineering experience. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors contribute to a streamlined event-analysis system that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet. Equally important, EMERALD introduces a recursive framework for coordinating the dissemination of analyses from the distributed monitors to provide a global detection and response capability that can counter attacks occurring across an entire network enterprise. Further, EMERALD introduces a versatile application programmers' interface that enhances its ability to integrate with heterogeneous target hosts and provides a high degree of interoperability with third-party tool suites.

TITLE

Gabriel

AUTHOR

Los Altos Technologies, Cupertino, CA

SOURCE

http://www.lat.com/gabe.htm

KEYWORDS

system monitoring

CONTACT INFORMATION

Richard Mahn
20813 Stevens Creek Blvd, Suite 275
Cupertino, CA 95014-2107
Phone: 800.999.UNIX
408.973.7700
Fax: 408.973.7707
Email: Majordomo@lat.com
URL: http://www.lat.com/gabe.htm

ABSTRACT

Gabriel is a SATAN detector, similar to Courtney. Available for Sun platforms, it is written entirely in C and comes prebuilt. As a public service, Los Altos Technologies, a provider of UNIX system security software, has developed and released this software. Gabriel gives the system administrator an early warning of possible network intrusions by detecting and identifying network probing. Gabriel is complete and ready to run. Los Altos Technologies is providing Gabriel to its customers and anyone else who wishes to use it at no charge. It is expected that any future updates, enhancements, and revisions will come from the users.

GrIDS

TITLE

GrIDS (Graph-based Intrusion Detection System)

AUTHOR

University of California at Davis

SOURCE

http://olympus.cs.ucdavis.edu/arpa/grids/welcome.html

KEYWORDS

anomaly detection, sniffers

CONTACT INFORMATION

Todd Heberlein
Security Lab
Department of Computer Science
2063 Engineering II
University of California, Davis
Davis, CA 95616-8562
Phone: 530.752.7004
Facx: n/a
Email: heberlei@cs.ucdavis.edu
URL: http://seclab.cs.ucdavis.edu/arpa/people/todd.html

ABSTRACT

GrIDS's core component is a graph-based language for analyzing network connection activity in a LAN-MAN sized system. The key point of GrIDS is to detect large-scale automated attacks on networked systems. The mechanism proposed is to build activity graphs. GrIDS contains a language for specifying how network connection activity is represented in graphical form, incorporating information from host-based IDS, network sniffers, and connection analysis components. The same language allows users to specify graphical structures that require notification of system administrators. This language is suitable for implementing network access control policies and identifying attack signatures.

BIBLIOGRAPHY

Staniford-Chen, S.; Cheung, S.; Crawford, R.; Dilger, M.; Frank, J.; Hoagland, J.; Levitt, K.; Wee, C.; Yip, R.; Zerkle, D.: GrIDS - A Graph Based Intrusion Detection System for Large Networks, Proc. of the 19th National Information Systems Security Conference, Baltimore, MD, Oct. 1996, 361 370.

TITLE

IDES/NIDES (Intrusion-Detection Expert System/Next-Generation IDES)

AUTHOR

SRI International, Menlo Park, CA

SOURCE

http://www.csl.sri.com/nides/index.html

KEYWORDS

anomaly detection, expert system, misuse detection, system monitoring

CONTACT INFORMATION

Phillip A. Porras
SRI International
Computer Science Laboratory
Attention: NIDES
333 Ravenswood Avenue
Menlo Park, CA 94025
Phone: 415.859.3232
Fax: 415.859.2844
Email: porras@csl.sri.com
URL: http://www.csl.sri.com/~porras

ABSTRACT

IDES is a real-time intrusion-detection expert system that observes user behavior on a monitored computer system and adaptively learns what is normal for individual users, groups, remote hosts, and the overall system behavior. Observed behavior is flagged as a potential intrusion if it deviates significantly from the expected behavior or if it triggers a rule in the expert-system rule base. NIDES is an expansion of IDES.

NIDES is a comprehensive intrusion-detection system that performs real-time monitoring of user activity on multiple target systems connected via Ethernet. NIDES runs on its own workstation (the NIDES host) and analyzes audit data collected from various interconnected systems, searching for activity that may indicate unusual and/or malicious user behavior. Analysis is performed using two complementary detection units: a rule-based signature analysis subsystem and a statistical profile-based anomaly-detection subsystem. The NIDES rule-base employs expert rules to characterize known intrusive activity represented in activity logs, and raises alarms as matches are identified between the observed activity logs and the rule encodings. The statistical subsystem maintains historical profiles of usage per user and raises an alarm when observed activity departs from established patterns of usage for an individual. The alarms generated by the two analysis units are screened by a resolver component, which filters and displays warnings as necessary through the NIDES host X-window interface.

The NIDES project acknowledges funding support from the following agencies: Department of the Navy, Federal Bureau of Investigation, National Security Agency, and Rome Laboritories.

BIBLIOGRAPHY

Anderson, D.; Lunt, T. F.; Javitz, H.; Tamaru, A.; Valdes, A.: Detecting Unusual Program Behavior Using the Stastistical Component of the Next-Generation Intrusion Detection Expert System (NIDES), SRI-CSL-95-06, SRI International, Menlo Park, CA, May 1995.

Anderson, D.; Frivold, Th.; Valdes, A.: Next-Generation Intrusion Detection Expert System (NIDES): A Summary, SRI-CSL-95-07, SRI International, Menlo Park, CA, May 1995.

TITLE

IDIOT (Intrusion Detection In Our Time)

AUTHOR

Sandeep Kumar and Eugene H. Spafford
Purdue University

SOURCE

ftp://coast.cs.purdue.edu/pub/doc/intrusion_detection/IDIOT_Users_Guide.ps

KEYWORDS

misuse detection

CONTACT INFORMATION

Eugene H. Spafford
Purdue University
1398 Computer Science Building
West Lafayette, IN, 47907-1398
Phone: 765.494.7825
Fax 765.494.0739
Email: spaf@cs.purdue.edu
URL: http://www.cs.purdue.edu/faculty/spaf.html

ABSRACT

IDIOT is Intrusion Detection In Our Time, a project to develop a new approach to efficient misuse detection methods. This work was started by Sandeep Kumar. He designed a new method of employing complex pattern matching to intrusion signatures. His design made use of a new classification of intrusion methods based on complexity of matching and temporal characteristics. He also designed a generic matching engine based on colored Petri nets.

BIBLIOGRAPHY

Crosbie, M.; Dole, B.; Ellis, T.; Krsul, I.; Spafford, E.: IDIOT - Users Guide, Technical Report TR-96-050, Purdue University, COAST Laboratory, Sept. 1996.

TITLE

Ifstatus

AUTHOR

David Curry

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/UNIX/ifstatus

KEYWORDS

anomaly detection

CONTACT INFORMATION

David Curry
International Business Machines Corporation
300 Long Meadow Road, Mail Stop 227
Sterling Forest, NY 10979 U.S.A.
Phone: 914.759.4452
Fax: 914.759.4326
Email: davy@vnet.ibm.com
URL: http://www.ers.ibm.com/~davy

ABSTRACT

Ifstatus checks network interfaces for promiscuous or debug mode in an attempt to determine if a sniffer is being run. This may indicate that an attacker has broken in and started a packet snooping program. Ifstatus is designed to be run out of cron.

Ifstatus checks all network interfaces on the system, and reports any that are in debug or promiscuous mode, which may be a sign of unauthorized access to the system.

If the -v option is specified, ifstatus will print the name of each interface and the hexadecimal representation of the interface's flags word.

Due to a bug in Solaris 2.3, ifstatus will not report an interface that is in promiscuous mode. A new version of ifstatus that will work on Solaris 2.3 is in development, but has not yet been released.

BIBLIOGRAPHY

SRI International. Improving the Security of Your UNIX System. Published as SRI International Technical Report No. ITSTD-721-FR-90-21, April 1990.

INTERNET SCANNER TOOLSET

TITLE

Internet Scanner Toolset

AUTHOR

Internet Security Systems, Atlanta, GA

SOURCE

http://www.iss.net/prod/isb.html

KEYWORDS

anomaly detection, vulnerability analysis

CONTACT INFORMATION

Patrick Taylor
41 Perimeter Center East, Suite 660
Atlanta, GA 30346
Phone: 770.395.0150
Fax: 770.395.1972
Email: info@iss.net
URL: http://www.iss.net

ABSTRACT

ISS's Internet Scanner Toolset is a security solution for intrusion detection and network vulnerability analysis and decision support. Internet Scanner tools directly address the single most important aspect of organizational network risk management-identifying and addressing technical vulnerabilities. The Internet Scanner set of tools perform scheduled and selective probes of a network's communication services, operating systems, key applications, and routers in search of those vulnerabilities most often used by individuals to probe, investigate, and attack the network. Internet Scanner then analyzes the vulnerability conditions and provides a series of corrective actions, trends analysis, conditional, and configuration reports and data sets. Internet Scanner consists of three integrated modules for scanning intranets, scanning firewalls, and scanning webservers. These modules are available singly as well as part of the Internet Scanner bundle.

BIBLIOGRAPHY

Internet Security Systems Profile by the Aberdeen Group. http://www.aberdeen.com/secure/profiles /iss/iss.htm. November 3, 1997.

INTOUCH INSA

TITLE

INTOUCH INSA - Network Security Agent

AUTHOR

Touch Technologies, Inc., San Diego, CA

SOURCE

http://www.ttisms.com/tti/nsa_www.html

KEYWORDS

anomaly detection, keystroke surveillance, misuse detection

CONTACT INFORMATION

Jim Geier
Touch Technologies, Inc.
9988 Hibert St. #310
San Diego, CA 92131
Phone: 800.525.2527
Fax: 619.566.3663
Email: sales@ttinet.com
URL: http://www.ttisms.com/tti/nsa_www.html

ABSTRACT

INTOUCH INSA provides network-wide surveillance. All network-based user activity is scanned, regardless of the computer manufacturer or operating system being used. Through the use of keystroke-level surveillance, INTOUCH INSA detects users not authorized to access a particular computer system and Users allowed to access a particular computer system, but engaged in unauthorized or suspicious activities. INTOUCH INSA has no impact on network or system performance. INTOUCH INSA requires no loading of software to any system, anywhere on the network. Even INTOUCH INSA's real-time display of user activity has absolutely no impact on network or system performance. INTOUCH INSA comes complete—-packaged as a turn-key system. Included in the package is a devoted, high-speed, 64-bit RISC system. Installation is quick and easy. INTOUCH INSA - Network Security Agent scans all user activity on your networks, 7 days a week, 24 hours a day. Whether the intrusion is from the outside (firewall failure) or from the inside (unauthorized insider activity), this detects the intrusion activity and takes manager-defined actions.

Running on a devoted, high-speed, 64-bit RISC system, INTOUCH INSA reads all network packets, reconstructs all user activity, and scans the activity for possible computer-use policy violations. The scanning is done automatically, in the background, and without any impact on the network. The patterns to be scanned for can be customized by the network security manager.

When a possible policy violation is detected by INTOUCH INSA, the network security manager is alerted. Once alerted, the network security manager can review the incident, and start a real-time display of the possible violator's session.

Capabilities include hosting on a single Digital AlphaStation for high-speed, real-time network traffic analysis and session reconstruction. This approach uses four detection techniques. These are attack signature recognition, anomaly detection, source/destination analysis, and network load analysis. Real-time and retrospective analysis is provided.

TITLE

ITA (Intruder Alert)

AUTHOR

AXENT Technologies, Inc., Rockville, MD

SOURCE

http://www.axent.com/product/ita/ita.htm

KEYWORDS

anomaly detection, audit-based detection, misuse detection

CONTACT INFORMATION

Jennifer Whipp
AXENT Technologies, Inc.
Headquarters
2400 Research Boulevard
Rockville, MD 20850
Phone: 301.670.3653
Fax: 301.330.5756
Email: info@axent.com
URL: http://www.axent.com/about/contact/contact.htm

ABSTRACT

ITA is used to detect intruders or abuse by analyzing audit data from the operating systems it supports. ITA detects intruders by rule or by exception. ITA is a rules engine; it processes the inputs it receives based on rules applied to the systems it is monitoring. Some rules may be designed to look at a specific sequence of events, called "footprints." If a particular footprint is detected, ITA can be programmed to take action to prevent any damage from occurring. Other rules detect behavioral anomalies within the system. These rules filter out normal activities, leaving the exceptions to be acted upon or investigated as needed. This anomaly type detection is often referred to as norm-based detection, or "baselining." ITA is deployed in three pieces, an interface console, a manager, and an agent. The interface and manager act as a configuration engine, allowing the user to easily configure the rules. Agents are intelligent processes or daemons that run on the local systems, executing the rules as configured by the user. Agents are registered to managers to provide a secure communications path. If a number of agents are registered to a manager, these agents can be organized into multiple domains. ITA has always produced results, usually in the form of catching hackers, abusers and intruders. Additionally, it has the capability to consolidate and filter events from several sources into one file. A new addition, ITA Graph, now can take that data and format it into easily understood graphs, charts and reports. Now users of ITA can do trend analysis, create bar chart or pie charts that reflect activity over time, or any number of other graphs via this utility. ITA Graph is based on a relational database that can import any ITA generated log file. It requires Windows 95 or Windows NT 3.51 or 4.0 to run. ITA monitors SNMP events. SNMP is an application layer protocol for the management of a TCP/IP internet consisting of network management stations called SNMP Managers communicating with network elements called SNMP Agents.

A wide range of networked devices have implemented SNMP Agent functionality including routers, bridges, switches, hosts, terminal servers, X terminals, even vending machines. Using ITA's new SNMP capabilities, traditional SNMP management stations can react to security threats through the ITA action list. This feature significantly extends the abilities of preexisting SNMP management stations such as HP's OpenView(tm) or IBM's TME/10 (Tivoli).

TITLE

Kane Security Monitor (KSM)

AUTHOR

Intrusion Detection Incorporated
New York, NY

SOURCE

http://www.intrusion.com/products/ksm.htm

KEYWORD

misuse detection, system monitoring

CONTACT INFORMATION

Daniel Dorr
Intrusion Detection, Inc.
217 E 86th St. Suite 213
New York, NY 10028
Phone: 212.348.8900.x302
Fax: 212.427.9185
Email: info@intrusion.com
URL: http://www.intrusion.com/contact.htm

ABSTRACT

The Kane Security Monitor is an intrusion detection system that provides sophisticated network security monitoring. Using artificial intelligence, the KSM identifies both subtle and obvious security violations caused by outside hackers or even inside authorized users. Once a violation has been identified, the system administrator or security officer is alerted with the details. Features are as follows: automatically identifies security violations; uncovers security break-ins before they occur; identifies password guessers, curious users, file browsers, compromised user IDs, password cracking attempts, network doorknob attacks, privileged ID abuse, data flooding, packet browsing and more; focuses on sensitive users, workstations and files. KSM also requires minimal setup time by using the built-in time saving self-populating database of expert security information. Security officers, auditors or LAN administrators can be automatically alerted about unauthorized access.

The KSM provides an enterprise-wide centralized collection facility for event logs otherwise stored separately on each machine, and the automated review of event logs for abuse patterns such as unauthorized activities and suspicious behavior by both outside hackers and inside authorized users. The KSM analyzes NT Security event logs on an enterprise-wide basis. The KSM's agent technology vigilantly monitors NT security event logs on thousands of NT servers and workstations. By using artificial intelligence from our proprietary SHADOWARETM technology, security event logs are scrutinized for abuse patterns including unauthorized activities and suspicious behavior from outside hackers and inside authorized users. This process automatically turns massive amounts of NT security event log data into concise security information. A network administrator or security officer can easily set a system warning when security events occur. For example, the administrator might want to be notified if a new administrative account is created or deleted, or if a user ID turned off the audit trail, reset a password or accessed the CEO's desktop and copied several sensitive files.

The KSM identifies any unusual activity on the network. By analyzing network activity, the KSM establishes a baseline for average network usage. When security activity exceeds the average, the KSM reacts. For example, if a particular user ID has a highly unusual number of login violations, the KSM will alert the security officer or system administrator via page, fax, e-mail or printout to investigate further.

The Kane Security Monitor identifies security break-in patterns including security attack profile, failed login attempts, failed file access attempts, browsing & curious users, denial of service, excessive privilege granting, ghost IDs, masquerading users, password cracking, administrative ID abuse, and supervisor abuse.

BIBLIOGRAPHY

"Intrusion Detection Inc. announces enhancements to KSA suite of network security products." March 6, 1997 New York, NY, http://www.intrusion.com/literature/strat97.htm

TITLE

md5check

AUTHOR

The University of California, Davis, CA

SOURCE

http://www.UNIX.digital.com/demos/freekit/docs/md5check

KEYWORDS

file integrity

CONTACT INFORMATION

Todd Heberlein
Security Lab
Department of Computer Science
2063 Engineering II
University of California, Davis
Davis, CA 95616-8562
Phone: 530.752.7004
Fax: n/a
Email: heberlei@cs.ucdavis.edu
URL: http://seclab.cs.ucdavis.edu/arpa/people/todd.html

ABSTRACT

md5check compares the MD5 checksums of several critical SunOS 4.x system files to a database of known good checksums. md5check will generate a report indicating which files did or did not match checksums in the database. A failed match does not necessarily indicate the presence of a trojan binary, instead, it simply means that the checksum was not found in the current checksum table. The file's authenticity should be verified against distribution media or local modifications. A correct match indicates that the corresponding file is free from tampering. This work was produced under the sponsorship of the U.S. Department of Energy under contract number W-7405-ENG-48.

NADIR

TITLE

NADIR (Network Anomaly Detection and Intrusion Reporter)

AUTHOR

Los Alamos National Laboratory
Los Alamos, NM

SOURCE

http://www.c3.lanl.gov/~gslentz/Web_projects/nadir.shtml

KEYWORDS

anomaly detection

CONTACT INFORMATION

Joseph Thompson
CIC-8, MS B272
Los Alamos National Laboratory
Los Alamos, NM 87545

Phone:	505.667.5553
Fax:	505.665.6333
Email:	jlt@lanl.gov
URL:	http://www.lanl.gov/ cgi-bin/phone/085768

ABSTRACT

NADIR is a rules-based expert system developed at Los Alamos to automatically detect intrusion attempts and other security anomalies on its large supercomputer network. In addition to monitoring the Cray supercomputer systems, NADIR also monitors network authentication (Kerberos) and mass file storage activity (Common File System). A client-server model is used, with UNIX-based workstations running Sybase providing the server application platform. Profiles and event history are maintained for each monitored system and for individual users, and rules are applied to these profiles to detect anomalous activities.

BIBLIOGRAPHY

Hochberg, J.; Jackson, K.; Stallings, C.; McClary, J.; DuBois, D.; Ford, J.: NADIR: An automated system for detecting network intrusions and misuse, Computers and Security 12(1993)3, May, 253 248

Jackson, K. A.: NADIR: A Prototype System for Detecting Network and File System Abuse, Proc. of the 7th European Conference on Information Systems, Nov. 1992.

Jackson, K.; DuBois, D. H.; Stallings, C. A.: An expert system application for network intrusion detection, Proc. of the 14th National Computer Security Conference, Washington, D.C., Oct. 1991, 215 225.

TITLE

NETMAN

AUTHOR

Mike Schulze and Craig Farrell
Curtin University of Technology

SOURCE

ftp://ftp.cs.curtin.edu.au/pub/netman/README

KEYWORDS

system monitoring

CONTACT INFORMATION

Mike Schulze
Curtin University of Technology
GPO Box U1987
Perth 6845
Western Australia
Phone: 61.8.9266.9266
Fax: n/a
Email: customer-service@curtin.edu.au
URL: http://www.cs.curtin.edu.au/~mike

ABSTRACT

The NETMAN package of network monitoring and visualization tools from Curtin University is a set of tools for monitoring and displaying network communications. Two of the tools provide a real-time picture of network communications, while the other provides retrospective packet analysis. These tools are designed to allow network managers to passively monitor a network and diagnose common network problems as quickly and efficiently as possible.

The tools include: (1) Etherman, an X11-based tool that displays a representation of real-time Ethernet communications. Network data are promiscuously received via a system "network tap" and summarized into useful statistics. These statistics are displayed in a graphical manner, to allow both experienced network managers and beginners insight as to how a network is being used. Etherman will also provide protocol summaries, usage statistics, and postscript(tm) snapshots of network activity. (2) Interman focuses on IP connectivity within a single segment. As with Etherman, this tool allows a real-time representation of network communications to be displayed. Interman employs the same methods of network data capture as Etherman, except only IP traffic is considered. Because IP is a network-level protocol, Interman will display multiple networks both local and remote. Protocol summaries, usage statistics and postscript snapshots are also available. (3) Packetman is a retrospective Ethernet packet analyzer. This tool allows the capture and analysis of an Ethernet packet trace. (4) Loadman is a network load monitor that utilizes the loading algorithm developed by Jeff Mogul at DEC Curtinstern Research Labs. (5) Geotraceman is a Visual Traceroute tool that build on traceroute. (6) Analyser is a network segmentation tool that recommends LAN partitioning configurations and visualizes them. At present, binaries for Sun SPARC (SunOS 4.1.x) and DEC-mips (Ultrix 4.2a and above) SGI IRIX 4.0X are available. Curtin has not finished Solaris or Dec Alpha binaries.

TITLE

NetRanger

AUTHOR

WheelGroup Corporation
San Antonio, TX

SOURCE

http://www.wheelgroup.com/netrangr/1netrang.html

KEYWORDS

anomaly detection, misuse detection, system monitoring

CONTACT INFORMATION

Joel McSarland
WheelGroup Corporation
13750 San Pedro, Suite 670
San Antonio, TX 78232
Phone: 210.494.3383
Fax: 210.494.6303
Email: info@wheelgroup.com
URL: http://www.wheelgroup.com/contact/1contact.html

ABSTRACT

NetRanger™ intrusion detection system from WheelGroup provides large-scale, real-time network security visibility for an enterprise by providing answers to the who, what, where, when, and how questions about the security activity on a network and the ability to dynamically respond to threats.

The NetRanger system consists of two elements: the NetRanger Sensor, located at network connections to be monitored, and a NetRanger Director, which is centrally located. The Sensor, either working independently or in conjunction with a network device such as a Cisco router, StorageTek NSG BorderGuard or Nortel Passport switch, analyzes the data traffic flowing in both directions across the connection. Looking at both the content and context of the datastream, NetRanger searches for signatures indicative of hacking attacks or other security violations. When a NetRanger Sensor detects an attack, it can immediately block it, depending on the requirements of the user, and can send a real-time alarm to the monitoring. The NetRanger Director is centrally located and can monitor the inputs of numerous sensors enterprise-wide, whether they are located at Internet connections, dial-up modem pools, network backbones, or local area network segments. The Director controls the configurations of each sensor, can upload new signatures as they are developed by WheelGroup's advanced research team, and receives and processes alarms from each sensor in a graphical format. Directors can also be arranged in a tiered fashion to control a virtually unlimited number of sensors.

With NetRanger, an organization can attain centralized network security "visibility" gained by monitoring connections of a geographically-distributed enterprise.

TITLE

NID (Network Intrusion Detector)

AUTHOR

Computer Security Technology Center
Livermore, CA

SOURCE

http://ciac.llnl.gov/cstc/nid/nid.html

KEYWORDS

anomaly detection, misuse detection

CONTACT INFORMATION

Joe Milner
Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550
Phone: 510.422.9839
Fax: 510.423.8988
Email: IPandC@llnl.gov
URL: http://ciac.llnl.gov/cstc/nid/nid.html

ABSTRACT

NID provides a suite of security tools that detect and analyze network intrusion. NID provides detection and analysis of intrusion from individuals not authorized to use a particular computer and from individuals allowed to use a particular computer, but who perform either unauthorized activities or activities of suspicious nature on it. The Network Intrusion Detector helps detect, analyze, and gather evidence of intrusive behavior on Ethernet and FDDI networks using the Internet protocol. NID is directly connected to the local area network it protects. It collects packets or statistics that cross a user-defined security domain. When threat patterns are recognized, NID signals the event locally and can save the suspicious session for later analysis or playback. NID operates passively on a stand-alone host rather than residing on the hosts it is protecting. NID provides an effective and inexpensive network intrusion detection capability, and combines three detection techniques: attack signature recognition, anomaly detection, and vulnerability risk model. Note that NID was formerly known as the Network Security Monitor (NSM) and was originally developed at the University of California at Davis.

NIDES/IDES

TITLE

IDES/NIDES (Intrusion-Detection Expert System/Next-Generation IDES)

AUTHOR

SRI International, Menlo Park, CA

SOURCE

http://www.csl.sri.com/nides/index.html

KEYWORDS

anomaly detection, expert system, misuse detection, system monitoring

CONTACT INFORMATION

Phillip A. Porras
SRI International
Computer Science Laboratory
Attention: NIDES
333 Ravenswood Avenue
Menlo Park, CA 94025
Phone: 415.859.3232
Fax: 415.859.2844
Email: porras@csl.sri.com
URL: http://www.csl.sri.com/~porras

ABSTRACT

IDES is a real-time intrusion-detection expert system that observes user behavior on a monitored computer system and adaptively learns what is normal for individual users, groups, remote hosts, and the overall system behavior. Observed behavior is flagged as a potential intrusion if it deviates significantly from the expected behavior or if it triggers a rule in the expert-system rule base. NIDES is an expansion of IDES.

NIDES is a comprehensive intrusion-detection system that performs real-time monitoring of user activity on multiple target systems connected via Ethernet. NIDES runs on its own workstation (the NIDES host) and analyzes audit data collected from various interconnected systems, searching for activity that may indicate unusual and/or malicious user behavior. Analysis is performed using two complementary detection units: a rule-based signature analysis subsystem and a statistical profile-based anomaly-detection subsystem. The NIDES rule-base employs expert rules to characterize known intrusive activity represented in activity logs, and raises alarms as matches are identified between the observed activity logs and the rule encodings. The statistical subsystem maintains historical profiles of usage per user and raises an alarm when observed activity departs from established patterns of usage for an individual. The alarms generated by the two analysis units are screened by a resolver component, which filters and displays warnings as necessary through the NIDES host X-window interface.

The NIDES project acknowledges funding support from the following agencies: Department of the Navy, Federal Bureau of Investigation, National Security Agency, and Rome Laboritories.

BIBLIOGRAPHY

Anderson, D.; Lunt, T. F.; Javitz, H.; Tamaru, A.; Valdes, A.: Detecting Unusual Program Behavior Using the Stastistical Component of the Next-Generation Intrusion Detection Expert System (NIDES), SRI-CSL-95-06, SRI International, Menlo Park, CA, May 1995.

Anderson, D.; Frivold, Th.; Valdes, A.: Next-Generation Intrusion Detection Expert System (NIDES): A Summary, SRI-CSL-95-07, SRI International, Menlo Park, CA, May 1995.

TITLE

NOCOL (Network Operations Center On-Line)

AUTHOR

JVNC-Net

SOURCE

http://www.mscs.mu.edu/contact.html

KEYWORDS

system monitoring

CONTACT INFORMATION

Dr. Douglas Harris
Department of Mathematics, Statistics, and Computer Science
Marquette University
P.O. Box 1881
Milwaukee, WI 53201-1881
Phone: 414.288.7573
Fax: 414.288.5472
Email: doug@mscs.mu.edu
URL: http://www.mscs.mu.edu/contact.html

ABSTRACT

NOCOL/NetConsole (Network Operations Center On-Line) is a network monitoring package that runs on UNIX platforms. NOCOL monitors network and system variables, such as ICMP or RPC reachability, RMON variables, nameservers, ethernet load, port reachability, host performance, SNMP traps, modem line usage, Appletalk and Novell routes/services, BGP peers. The software is extensible, and new monitors can be added easily. The software consists of a number of individual, standalone monitoring agents that poll the various network and system parameters and put them into a common data format. All the monitors have a common display and postprocessing interface (such as logging, notification). The design allows running just one set of monitoring agents and any number of display agents, and all of the displays see the same consistent set of data. Additionally, each event is assigned a severity (determined by comparing against user defined threshold values) that is gradually escalated, thus preventing false alarms and a customized priority notification based on the severity. There are four severity levels ranging from Critical through Info, and each event typically steps through each one of these severities until it reaches its maximum allowed level. The display uses UNIX "curses" screen management and can thus run on a large variety of terminals. The user running the display can select the minimum display severityonly events above this minimum severity level are displayed.

To date, the various monitoring agents developed are: IP ICMP monitor (using IP "multiping"), OSI reachability monitor (using OSI ping), RPC portmapper monitor (using "rpcping"), Ethernet load (bandwidth and pps), TCP port monitor, UNIX host performance (disks, memory, swap, load, nfs, collisions), SNMP variables monitor (RMON, Cisco router, terminal server), TCP data throughput monitor, Nameserver (named), SNMP traps, Usage of terminal server modem lines (busy lines), Appletalk route monitor (for Cisco routers), Novell service monitor, and BGP peer status.

TITLE

Noshell

AUTHOR

Michele D. Crabb

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/UNIX/noshell/src

KEYWORDS

system monitoring

CONTACT INFORMATION

Michele D. Crabb
Cisco Systems, Inc.
1160 West Swedesford Road
Suite 100
Berwyn, PA 19312
Phone: 610.695.6000
Fax: 610.695.6006
Email: cs@cisco.com
URL: http://www.cisco.com/warp/public/437/Service.html

ABSTRACT

This program is designed to provide the system administrator with additional information about who is logging into disabled accounts. Traditionally, accounts have been disabled by changing the shell field of the password entry to "/bin/sync" or some other benign program. Noshell provides an informative alternative to this method by specifying the Noshell program as the login shell in the password entry for any account that has been disabled.

Noshell has been tested and configured for the following types of systems: 1) a VAX 780 running 4.3 BSD; 2) an Amdahl 5880 running UTS580-1.2.3 (with 4.3 networking code); 3) a SPARCstation running 4.0.3c; 4) Sun3's running 4.0.1; 5) Silicon Graphics 4D series running Rel. 3.2; 6) Silicon Graphics IRIS running Rel. 3.5; 7) a VAX 6320 running Ultrix-32 V3.1.

If Noshell is specified in the shell field of a password entry, the following information will be captured when someone logs into disabled account: 1) remote user name, if available in the user's environment vector; 2) remote host name, if available in the utmp entry; 3) remote Internet address, if inet_ntoa or nslookup is available; 4) time of login; 5) tty line user is attached.

There are compile-time options that provide one or all of the following notification capabilities: 1) Mail a message to a system administrator. In addition to the above information, the name of the system and the local user ID use will be included in the mail message. This is specified by defining "MAIL_MSG" and "WATCHER" in the header file. 2) Log information to a system log file using the syslogd daemon process. The log facility is specified in the noshell.h file. This is specified by defining "SYSLOG" and "LOG_FACIL" in the header file. 3) Display a message to the user who has logged in. The message can be a predefined message stored in a file or a short message such as "Your account has been disabled at this time." This is specified by defining "PRINT_MSG" and "USER_MSG" in the header file.

NSM

TITLE

NSM (Network Security Monitor)

AUTHOR

University of California at Davis

SOURCE

http://olympus.cs.ucdavis.edu/arpa/grids/welcome.html

KEYWORDS

system monitoring

CONTACT INFORMATION

Todd Heberlein
Security Lab
Department of Computer Science
2063 Engineering II
University of California, Davis
Davis, CA 95616-8562
Phone: 530.752.7004
Fax: n/a
Email: heberlei@cs.ucdavis.edu
URL: http://seclab.cs.ucdavis.edu/arpa/people/todd.html

ABSTRACT

NSM (Network Security Monitor) is an intrusion detection system developed at the University of California-Davis. NSM is a network-based IDS that does not use or analyze the host machine(s) audit trails. It monitors network traffic in order to detect intrusions. Because networkbased attacks are expected to be prevalent due to the mushrooming of the Internet, NSM could prove to be a valuable tool to detect intrusive activity.

NSM has several perceived advantages. First, the IDS gets instantaneous access to network data. Second, the IDS is hidden from the intruder because it is passively listening to network traffic; therefore, it cannot be shut off or its data compromised. Finally, the IDS can be used with any system because it monitors network traffic, protocols for which (TCP, UDP, etc.) are standardized. There is no problem with different audit files, for example. Researchers at Purdue University are working on several issues in intrusion detection. Crosbie and Spafford propose to build an IDS using Autonomous Agents. Instead of a single large IDS defending a system, they propose an approach where several independent, small processes operate while cooperating in maintaining the system. The advantages claimed for this approach are efficiency, fault tolerance, resilience to degradation, extensibility, and scalability. The foreseen drawbacks include the overhead of so many processes, long training times, and the fact that if the system is subverted, it becomes a security liability. An interesting possibility they raise is that of an active defense, that can respond to intrusions actively instead of passively reporting them (it could kill suspicious connections, for example).

BIBLIOGRAPHY

Heberlein, L. T.; Levitt, K. N.; Mukherjee, B.: A Method to Detect Intrusive Activity in a Networked Environment, Proc. of the 14th National Computer Security Conference, Washington D.C., Oct. 1991, 362371.

Heberlein, L. T.; Dias, G. V.; Levitt, K. N.; Mukherjee, B.; Wood, J.: Networks Attacks and an Ethernet-based Network Security Monitor, Proc. of the 13th DOE Security Group Conference, Augusta, GA, May 1990.

Heberlein, L. T.; Dias, G. V.; Levitt, K. N.; Mukherjee, B.; Wood, J.; Wolber, D.: A Network Security Monitor, Proc. of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, May 1990, 296304.

POLYCENTER

TITLE

POLYCENTER Security ID (POLYCENTER Security Intrusion Detector)

AUTHOR

Digital Equipment Corporation
Maynard, MA

SOURCE

http://www.digital.com/info/security/id.htm

KEYWORDS

misuse detection, system monitoring

CONTACT INFORMATION

Jim Burton
Digital Equipment Corporation
111 Powdermill Road
Maynard, MA 01754-1418
Phone: 603.884.4632
Fax: 1.800.676.7517
Email: polycenter@digital.com
URL: http://www.digital.com/misc/contacts.txt.html#US

ABSTRACT

POLYCENTER Security Intrusion Detector (POLYCENTER Security ID) is a real-time security monitoring application developed by Digital Equipment Corporation. It performs knowledge-based analysis of audit data to recognize and respond to simple security-relevant events. If suspicious activity is discovered, POLYCENTER Security ID respondS by sending an alert to the system manager and possibly shutting down the suspicious process if warranted. POLYCENTER Security ID supports the monitoring of a single host running either the OpenVMS, Digital UNIX, ULTRIX, or SunOS operating systems.

The POLYCENTER is a further development of DECinspect Intrusion Detector.

TITLE

RealSecure

AUTHOR

Internet Security Systems, Inc.,
Atlanta, GA

SOURCE

http://www.iss.net/prod/rs.html

KEYWORDS

system monitoring, vulnerability analysis

CONTACT INFORMATION

Patrick Taylor
41 Perimeter Center East, Suite 660
Atlanta, GA 30346
Phone: 770.395.0150
Fax: 770.395.1972
Email: info@iss.net
URL: http://www.iss.net/prod/rs.html

ABSTRACT

RealSecure is an automated, real-time network attack recognition and response system. RealSecure acts like a sniffer, unobtrusively analyzing packets of information as they travel across the network, and interpreting hostile activity on the network by recognizing the network traffic patterns that indicate attacks. When a vulnerability is exploited or an attack is recognized, the administrator is alerted via email, and an alarm is displayed on the management console. In addition, the attack can be terminated automatically, logged to a database, or recorded for later playback. RealSecure's distributed architecture allows installation of attack monitor engines throughout an enterprise network, so that attacks can be seen and stopped from inside as well as outside the network perimeter.

RealSecure(TM) is a real-time, automated attack recognition and response system. This system rests on the network, monitoring the network traffic stream looking for attacks and unauthorized access attempts. When RealSecure detects an attack, it may respond in a variety of ways, including logging the connection, notifying the network administrator, and killing the connection automatically.

RealSecure recognizes two types of network occurrences: One type is attacks, and involves network activity patterns indicating that someone may be engaged in unauthorized or undesirable activity involving the systems and/or data on the network. Examples of these include SATAN scans, ping floods, WinNuke, SYN floods, IP half scans, and attempts to obtain unauthorized root access. Misuse, the other type of occurrence, involves non-attack network activity that violates stated security or appropriate use policy. Examples of these include HTTP activity analysis of access to Windows shares, and email session decoding.

RealSecure has the capability to filter and monitor any TCP/IP protocol. The network administrator can configure RealSecure to filter by protocol (TCP, UDP, ICMP), source port, destination port, source IP address, and/or destination IP address. RealSecure can interpret the following network services: web surfing, email, file transfer, remote login, chat, and talk. In addition, RealSecure can monitor and decode Microsoft CIFS/SAMBA traffic for Windows networking environments.

RealSecure is installed on a host having a network adapter card. RealSecure places the adapter card in promiscuous mode so that it receives all the traffic on the local network segment. If a packet meets the filter criteria currently in force, it is parsed by the decode and attack recognition logic. Each active session is maintained and tracked, so attack patterns that span many packets can be detected. With this action, when an "questionable activity" is detected, the appropriate reactions can be taken. The actions taken upon detection of an attack or unauthorized activity are determined by the administrator. The administrator may choose from the following options: terminate the attack immediately; send an alarm to the management console indicating that the event occurred; log the event, including date, time source, destination, description, and data associated with the event; view the raw content of the session in real-time (or record for later playback); email a notification to the administrator; execute a user-specified program.

Currently, RealSecure is supported on the following platforms: Windows NT® 4.0, Solaris (SPARC) 2.4 or later, SunOS 4.1.3 or later, and Linux 1.3.x. RealSecure has been certified for 10-Mbps networks. ISS will be adding support for 100-Mbps technologies (i.e., FDDI, Fast Ethernet) very shortly, with support for additional networking topologies to follow.

RealSecure has two components and uses a distributed architecture. The RealSecure engine performs the filtering and monitoring functions on a given network segment. The RealSecure management console displays alarms, consolidates engine data, provides report generation capabilities, and acts as a centralized engine management point.

The authentication scheme is SKID-3. The management console provides a list of the engines that it manages along with a pass phrase used to authenticate data from each engine. Each engine contains a similar list for the management console. When one side wants to send a message to the other, the pass phrase is appended to the data, an MD5 checksum is calculated for the entire data set, and the checksum is attached to the packet (without the pass phrase). The entire message is encrypted and sent out over UDP. Upon receiving the message, the other side of the connection will decrypt the data field, remove the checksum, attach the pass phrase, calculate an MD5 checksum, and compare with the checksum received. If they match, the message is authenticated. The current encryption scheme is a fully exportable ISS proprietary encryption method. RealSecure is scheduled to use a modular, standard DES-or-better encryption scheme in the next major release.

TITLE

SecureNet PRO

AUTHOR

MimeStar, Inc.,
Blacksburg, VA

SOURCE

http://www.MimeStar.com/secmain.htm

KEYWORDS

keyword-level surveillance, system monitoring

CONTACT INFORMATION

Elliot Turner
MimeStar, Inc.
Blacksburg, VA
Phone: 540.953.3006
Fax: 540.953.1097
Email: MimeStar@MimeStar.com
URL: http://www.mimestar.com/secids.htm

ABSTRACT

SecureNet PRO is a complete network security system. It is one of few available systems that combines several key technologies, including session monitoring, firewalling, hijacking, and keyword-based intrusion detection.

Hacking attempts are detected and responded to in real-time, using SecureNet's advanced integrated intrusion detection system. Suspicious connections can be automatically killed or logged for later playback. Also, network administrators can be notified of all suspicious events via email.

SecureNet PRO also offers advanced intrusion response, using a technique known as TCP hijacking. Hijacking allows the administrator to instantly seize the connection of any user on his local area network. The user remains completely locked out while the administrator performs actions such as damage control or evidence collection.

SecureNet PRO is one of the few products available that offer automatic keystroke monitoring of all connections passing through the network. This can be used to detect suspicious/illegal activity, profanity, and computer usage policy violations. SecureNet PRO can automatically log, terminate, or notify the administrator after detecting any suspicious activity.

SecureNet PRO offers user-definable automated keyword monitoring to detect intruders. Other programs detect only a few hard-coded vulnerabilities, while SecureNet PRO detects dozens of attacks against a wide variety of different operating systems. New attack signatures are distributed to customers as they are made available, allowing SecureNet PRO to protect a network against even the latest security vulnerabilities. Attack detection for multiple operating systems in combination with periodic attack signature updates make SecureNet PRO a truly versatile network security solution.

When a network attack is detected, SecureNet PRO can automatically respond by killing suspicious connections, notifying security personnel via email, or logging any associated network activity for later review. This allows a network to be protected 24 hours a day 7 days a week, even when the network administrator is not present.

TITLE

Stake Out

AUTHOR

Harris Corporation
Melbourne, FL

SOURCE

http://www.stakeout.harris.com/

KEYWORDS

anomaly detection, misuse detection, system monitoring

CONTACT INFORMATION

Terry Beard
Harris Corporation
Telecommunication Systems & Services
1025 West NASA Blvd.
Melbourne, FL 32919
Phone: 407.724.3335
Fax: 407.724.3947
Email: stakeout@harris.com
URL: http://www.stakeout.harris.com

ABSTRACT

Stake Out is an intrusion detection and notification software that will detect many of the techniques used to compromise networkattached systems. Stake Out categorizes incidences as intrusions, probes, denial of service, and brute force attacks. Licensed customers automatically receive frequent updates to the detection module as new exploits of vulnerabilities can be identified.

Corporate incident response teams can be immediately alerted to potential network security events as Stake Out continues to log activity between the attacking and targeted hosts.

Stake Out monitors network traffic and detects intrusive or suspicious activity as it occurs on the wire. Upon detection, Stake Out will trigger a preconfigured alarm to the console, to Harris Network Management, any SNMP compliant network manager, or any combination of the three. When an alert has been triggered, an evidence log is created that captures all traffic to and from the identified attacking IP address and/or the targeted IP address. Stake Out can be run as a fully self-contained workstation and includes a graphical user interface to show the current state of an incident as well as the historical account of detected events. On the larger scale, Stake Out offers seamless integration into the world of network management.

BIBLIOGRAPHY

Harris Corporation: Stake Out. Network Surveillance, White Paper, 1996.

STALKER

TITLE

Stalker

AUTHOR

Haystack Laboratories, Inc.
Austin, TX

SOURCE

http://www.haystack.com/prodfr.htm

KEYWORDS

misuse detection

CONTACT INFORMATION

Fred Pinkett
Haystack Labs, Inc.
10713 RR 620 North, Suite 512
Austin, TX 78726

Phone:	617.239.8092
Fax:	512.918.1265
Email:	sales@haystack.com
URL:	http://www.haystack.com/contfr.htm

ABSTRACT

Stalker is a commercial, off-the-shelf security software designed to detect and respond to UNIX system misuse. Stalker identifies intruders and internal misuse by analyzing audit trail data and reporting on suspicious user and system activities. A misuse detector analyzes the audit trail data, looking for events that correspond to known attack techniques or known system vulnerabilities. A querying and reporting facility reduces the volume of audit trail data to find only the audit records of interests. The collection and storage of audit trails from multiple UNIX systems are managed on a single server by an audit control and storage manager. Stalker is available for Sun Microsystems, IBM, SCO UNIXWare, and HP UNIX systems, and supports Motif, CDE, and OpenLook.

BIBLIOGRAPHY

Smaha, S. E.; Winslow, J.: Misuse detection tools, Computer Security Journal 10(1994)1, Spring, 39 49.

TITLE

Swatch

AUTHOR

Stephen Hansen and Todd Atkins
Stanford University

SOURCE

http://star-www.rl.ac.uk/~cac/security/ssn67.htx/node19.html

KEYWORDS

misuse detection, system monitoring

CONTACT INFORMATION

Stephen Hansen
3rd Floor, Sweet Hall
590 Escondido Mall
Stanford University
Stanford, CA 94305-3090
Phone: 650.723.2911
Fax: 650.725.9121
Email: security@Stanford.EDU
URL: http://www-leland.stanford.edu/group/itss-ccs/security/

ABSTRACT

Swatch (Simple WATCHer) is a program for UNIX system logging and management developed at the Electrical Engineering Computer Facility at Stanford University. Swatch was designed to keep system administrators from being overwhelmed by large quantities of log data. Swatch can monitor information as it is being appended to a log file and alert system administrators immediately to serious system problems as they occur.

Swatch is a system for monitoring events on a large number of systems. It modifies certain programs to enhance their logging capabilities and software to then monitor the system logs for "important" messages. Modern UNIX systems can log a variety of information concerning the health and status of their hardware and operating system software, but are generally not configured to do so. Also, with a large network, a system administrator must often monitor several log files. Swatch is a utility that allows a system manager to log critical system and security related information to a dependable, secure, central logging host system. Swatch monitors log files and acts to filter out unwanted data and take one or more userspecified actions (ring bell, send mail, execute a script, etc.) based upon patterns in the log. This is useful when logging to a central host in conjunction with tcpwrappers to provide extra logging information.

TITLE

Tripwire

AUTHOR

Purdue University

SOURCE

http://www.cs.purdue.edu/

KEYWORDS

file integrity

CONTACT INFORMATION

Marlene G. Walls
Purdue University
1398 Computer Science Building
West Lafayette, IN, 47907-1398
Phone: 765.494.7805
Fax: 765.494.0739
Email: walls@cs.purdue.edu
URL: http://www.cs.purdue.edu/people/walls

ABSTRACT

Tripwire checks file and directory integrity. This utility compares a designated set of files and directories to information stored in a previously generated database. Any differences are flagged and logged, including added or deleted entries. When run against system files on a regular basis, Tripwire enables the user to view changes in critical system files and to immediately take appropriate damage control measures.

T-SIGHT

TITLE

T-sight

AUTHOR

En Garde Systems, Inc.
Albuquerque, NM

SOURCE

http://www.engarde.com/software/t-sight/index.html

KEYWORDS

system monitoring

CONTACT INFORMATION

Susan Carr
En Garde Systems, Inc.
One Executive Center
8500 Menaul NE, Ste A-335
Albuquerque, NM 87112
Phone: 505.275.8655
Fax: 505.275.8482
Email: spec@engarde.com
URL: http://www.engarde.com/contact.html

ABSTRACT

T-sight is designed to bring intrusion investigation and network data interpretation to a new level of sophistication by supplying an advanced method of visualizing the traffic and data transiting a network. The visualization is enacted through a unique framework with default risk settings. The built-in settings evaluate the risk of certain transactions, and the results of the evaluation are displayed as part of the connection/transaction data that can either be logged or viewed during real-time monitoring.

This evaluation, or "risk level", is meant to assist the user with determining which transactions warrant further inspection, and supports manual intrusion detection. In contrast, automated intrusion detection relies on flags generated by a static list of "signature" attacks. Although this feature is useful, it cannot keep pace with constantly changing security threats. To combat intruders at the highest level, administrators must be able to interpret threatening data.

Control is also an essential part of computer security. T-sight offers a system administrator the ability to prioritize the information provided by the program. This is accomplished by sorting, moving, or eliminating the connection data using the Main Window interface.

T-sight also has a customizable alarm system, a feature that can aid administrators who may not always have the time to actively monitor their network. By engaging this function, the user can indicate which activities should trigger alarms and how they would like to be alerted, therefore gaining control over what is considered suspicious activities by the program.

T-sight includes extensive logging and reporting features that offer advanced ways to analyze and define abuse or misuse. To ease the burden of heavy traffic volume, the filter and purge sections of the program can eliminate unnecessary data.

TITLE

UNICORN (Unicos Realtime NADIR)

AUTHOR

Los Alamos National Laboratory
Los Alamos, NM

SOURCE

http://www.EnGarde.com/~mcn/unicorn.html

KEYWORDS

audit-based detection

CONTACT INFORMATION

Susan Carr
En Garde Systems, Inc.
One Executive Center
8500 Menaul NE, Ste A-335
Albuquerque, NM 87112
Phone: 505.275.8655
Fax: 505.275.8482
Email: spec@engarde.com
URL: http://www.engarde.com/contact.html

ABSTRACT

UNICORN (Unicos Realtime NADIR) is an expansion on the NADIR project. Unicorn will accept audit logs from Unicos (Cray UNIX), Kerberos, and a common file system, then analyze them and attempt to detect intruders in realtime. Because UNICORN was designed for Kerberos and UNIX, the design can be applied to many other network configurations. UNICORN was presented at Supercomputing '95 in San Diego, CA.

BIBLIOGRAPHY

Christoph, G. G.; Jackson, K. A.; Neumann, M. C.; Siciliano, Ch. L. B.; Simmonds, D. D.; Stallings, C. A.; Thompson, J. L.: UNICORN: Misuse Detection for UNICOS, Proc. of Supercomputing '95, San Diego, CA, (published on CD-ROM).

Jackson, K.; Neumann, M.; Simmonds, D.; Stallings, C.; Thompson, J.; Christoph, G.: An Automated Computer Misuse Detection System for UNICOS, Proc. of the Cray Users Group Conference, Oct. 1994.

USTAT

TITLE

USTAT (UNIX State Transition Analysis Tool)

AUTHOR

Phillip A. Porras

SOURCE

http://www.cs.ucsb.edu/TRs/TRCS93-26.html

KEYWORDS

misuse detection, state transition analysis

CONTACT INFORMATION

Richard A. Kemmerer
Department of Computer Science
University of California Santa Barbara
Santa Barbara, CA 93106-5110
Phone: 805.893.4232
Fax: 805.893.8553
Email: kemm@cs.ucsb.edu
URL: http://www.cs.ucsb.edu/~kemm/

ABSTRACT

Developed as a thesis, this link presents the design and implementation of a real-time intrusion detection tool, referred to as USTAT, State Transition Analysis Tool for UNIX. The original design was first developed by Phillip A. Porras and presented as STAT, State Transition Analysis Tool. In STAT, a penetration is identified as a sequence of state changes that lead the computer system from some initial state to a target compromised state.

The author of this document has developed the first prototype, USTAT, for UNIX, in particular for SunOS 4.1.1. USTAT makes use of the audit trails that are collected by the C2 Basic Security Module of SunOS and it keeps track of only those critical actions that must occur for the successful completion of the penetration. This approach differs from other rule-based penetration identification tools that pattern match sequences of audit records.

BIBLIOGRAPHY

Illgun, K.; Kemmerer, R. A.; Porras, P. A.: State transition analysis: A rule-based intrusion detection approach, IEEE Transactions on Software Engineering (1995)3, 181199.

Ilgun, K.: USTAT: A Real-time Intrusion Detection System for UNIX, Proc. of the IEEE Computer Society Symposium on Research in Security and Privacy, May 1993, Oakland, CA, 16-28.

TITLE

WatchDog

AUTHOR

Fischer International Systems Corporation,
Naples, FL

SOURCE

http://www.infstream.com/WatchDogDoc.html

KEYWORDS

system monitoring

CONTACT INFORMATION

Ron Buehrer
3506 Mercantile Avenue
Naples, FL 34104
Phone: 804.527.1507
Fax: 804.527.1540
Email: Ron.Buehrer@fisc.com
URL: http://www.fisc.com/store/wd.html

ABSTRACT

WatchDog enhances system security by monitoring and managing the SunOS audit trail produced by the system's C2 security features and responding in real time to events that appear. The audit trail is stored as audit records in a series of files. The WatchDog application is a Motif graphical user interface (GUI) consisting of a main panel and various dialogs. All WatchDog functionality is accessed through the GUI. The actual real-time processing of the audit trail is done by the WatchDog Processor (WDP) whose operation is controlled through the Control dialog of the GUI. The WDP monitors the audit trail, looking for new audit records and checking them against events of interest of all active alarms. An alarm triggers when the WDP detects one or more occurrences of the alarm's events of interest, which signals the WDP to execute the alarm's responses. The WDP performs audit trail management when there are no new audit records to process. WatchDog is currently available for machines running SunOS 4.1.2+. The security service must also be installed so that an audit trail can be produced by the operating system.

TITLE

WebStalker Pro

AUTHOR

Haystack Laboratories, Inc.

SOURCE

http://www.haystack.com/prodfr.htm

KEYWORDS

misuse detection

CONTACT INFORMATION

Fred Pinkett
Haystack Labs, Inc.
10713 RR 620 North, Suite 512
Austin, TX 78726
Phone: 617.239.8092
Fax: 512.918.1265
Email: sales@haystack.com
URL: http://www.haystack.com/contfr.htm

ABSTRACT

WebStalker-Pro is a software-based, automated management tool that patrols the perimeter of the Web site and protects the integrity of the Web server.

WebStalker-Pro manages and controls access to the contents of a Web site by allowing only authorized individuals to modify the content files. WebStalker-Pro catches outsiders and insiders alike who may be attempting to modify Web sites, and either alerts the system manager or removes them.

Based on the user's responses to a quick, yet comprehensive, online interview, WebStalker automatically builds and enforces Web site security policy. The program includes a constantly updated, extensive database of ways to break into Web sites.

WebStalker-Pro can watch all Web and non-Web accesses, all processes, and all changes to Web and other files; notify in real-time through SNMP, pager, or email when anything suspicious occurs on a Web server; protect the network by automatically stopping unauthorized activities; ensure that a Web site is always available and accessible; and automatically restart server software if it goes down for any reason.

TITLE

X Connection Monitor

AUTHOR

der Mouse

SOURCE

http://www.cs.purdue.edu/

KEYWORDS

system monitoring

CONTACT INFORMATION

Marlene G. Walls
Purdue University
1398 Computer Science Building
West Lafayette, Indiana, 47907-1398

Phone:	765.494.7805
Fax:	765.494.0739
Email:	walls@cs.purdue.edu
URL:	http://www.cs.purdue.edu/people/walls

ABSTRACT

This program monitors X connections. It uses RFC931 to display usernames, when the client host supports RFC931. It allows the user to freeze and unfreeze connections, or kill them, independent of the client, and independent of the server. The KillClient request can be used to forcibly disconnect a client from the server, but only if the client has created a resource, that neither xkey nor crowbar does. The program monitors the connection, and if it sees certain dubious requests, currently configurable only by hacking on the source, it displays a menu that enables the user to allow the request, have it replaced with a no operation request, or kill the connection. The dubious requests are, at present, requests to change the host access list, requests to enable or disable access control, and Change Window Attributes requests operating on non-root windows not created by the same client.